FortiAnalyzer

Threat Report

Report Date: 2013-10-19

Data Range: 2013-10-12 00:00 - 2013-10-18 23:59 CEST (FAZ local)

FORTINET

Fortinet Inc. All Rights Reserved.

Table of Contents

Attacks 1
- Top Attack Victims 1
- Top Attack Sources 1

Virus 1
- Top Virus Victims 1
- Top Viruses by Name 1

Web Filter 1
- Top Web Users by Blocked Requests 1
- Top Web Users by Allowed Requests 1
- Top Blocked Websites by Requests 1
- Top Allowed Websites by Requests 1
- Top Blocked Web Categories 2
- Top Allowed Web Categories 2
- Web Activity Summary by Requests 2

Attacks

Top Attack Victims

No matching log data for this report

Top Attack Sources

No matching log data for this report

Virus

Top Virus Victims

Virus Victims	Occurrences
198.18.0.17	2

Top Viruses by Name

Virus Name	Occurrences
EICAR_TEST_FILE	2

Web Filter

Top Web Users by Allowed Requests

User (or IP)	Hostname (or Mac)	Requests
198.18.1.11		1.27 K
198.18.3.2		367
198.18.0.18	wsmacpro2	310
198.18.0.17	SatellitePro770	241
198.18.3.5		99
198.18.0.17		81
198.18.0.13	00:0c:29:bc:42:66	55
198.18.3.4		48
198.18.0.17	e8:40:f2:89:7b:a1	36
198.18.0.12	00:0c:29:36:5c:0f	8

Top Web Users by Blocked Requests

User (or IP)	Hostname (or Mac)	Requests
198.18.0.18	wsmacpro2	281
198.18.1.11		31
198.18.0.17		3
198.18.3.5		2
198.18.0.17	e8:40:f2:89:7b:a1	1
198.18.3.4		1

Top Allowed Websites by Requests

Website	Requests
tools.cisco.com	107
news-tags.cisco.com	105
www.cisco.com	98
safebrowsing.clients.google.com	90
safebrowsing-cache.google.com	79
tools-tags.cisco.com	61

Top Blocked Websites by Requests

Website	Requests
notify10.dropbox.com	168
ui.skype.com	107
46.165.192.221	31
r8---sn-nfpnnjvh-9anl.c.pack.google.com	4
www.sex.com	3
www.eicar.org	1

Top Allowed Websites by Requests (contd)

Website	Requests
partners-tags.cisco.com	61
h20566.www2.hp.com	59
www.fortiguard.com	55
cisco-tags.cisco.com	52

Top Blocked Websites by Requests (contd)

Website	Requests
www.classicshell.net	1
versioncheck.busymac.com	1

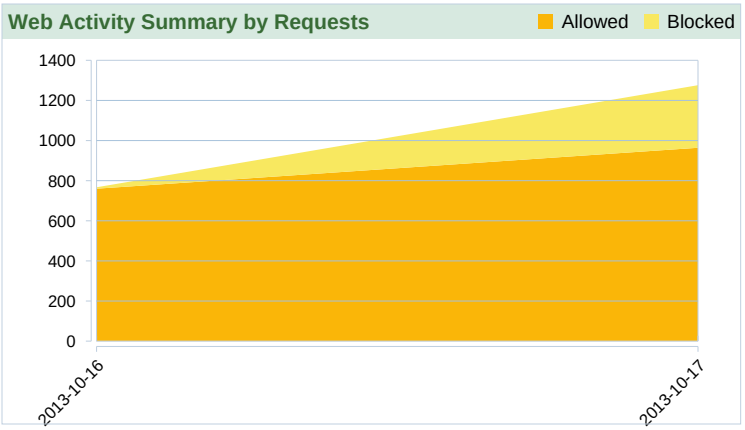
Top Allowed Web Categories

Categories	Requests
Information Technology	547
Search Engines and Portals	203
Business	106
Content Servers	68
Advertising	41
Reference	25
Web Hosting	15
Social Networking	13
Shopping and Auction	12
Information and Computer Security	8

Top Blocked Web Categories

Categories	Requests
File Sharing and Storage	168
Internet Telephony	107
Malicious Websites	32
Freeware and Software Downloads	6
Pornography	3

Web Activity Summary by Requests



Appendix A

Devices: alsochlu-sg0e0-root